ABSTRACT

A system allowing a participant to participate anonymously in a plurality of sessions but to be detected that the same participant has participated more than once in the same session is disclosed. The participant authorizes individual data using secret information depending on session-related information. The reception subsystem determines whether received data is anonymous participation data authorized by the participant subsystem and further determines whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem. The anonymous signature may include data generated by raising a session-dependent base to a power dependent on the secret information.